TODAY

* SIS problem
* Leftover Hash Lemma
* Collision-resistant hashing

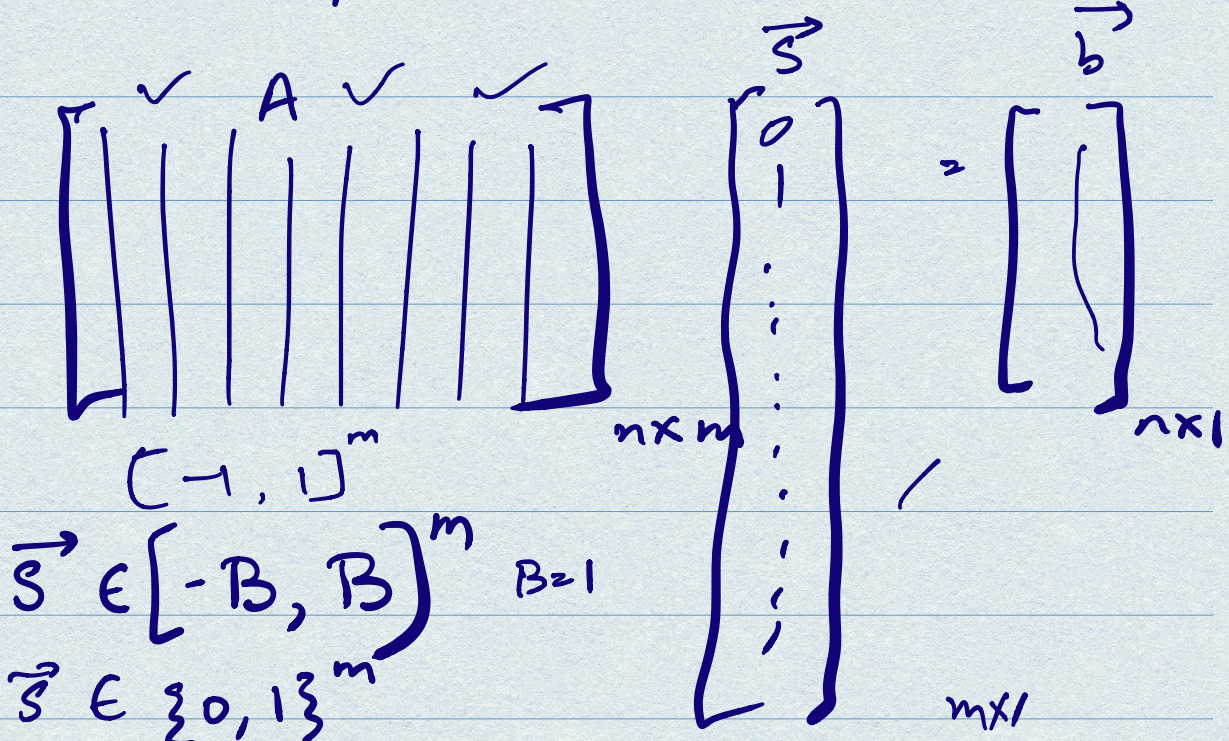
SIS Problem

(Inhomogenous SIS)

$$A \xleftarrow{\$} \mathbb{Z}_q^{n \times m}, \quad \vec{b} \xleftarrow{\$} \mathbb{Z}_q^{n}$$

Problem: Find $\vec{s}_{m \times 1}$ s.t.

$$A\vec{s} = \vec{b}$$



SIS Hardness Assumption:

$\forall$ nuPPT M,

$$\Pr_{\substack{A \leftarrow \mathbb{Z}_q^{n \times m} \\ \vec{b} \leftarrow \mathbb{Z}_q^{n}}} \left[M(A, \vec{b}) \text{ outputs } \vec{s} \in [-B, B] \text{ such that } A\vec{s} = \vec{b} \right] = \text{negl}(n)$$

$(2B+1)^m \gg q^n$: $3^m \gg q^n$

$m \sim O(n \log q)$ Eg. $B = 1$.

OWF. $f\left(A \in \mathbb{Z}_q^{n \times m}, \vec{s} \in [-B, B]^m\right) \rightarrow \left(A, A \cdot \vec{s}\right)$

If $\forall$ nuPPT $\mathcal{A}$,

$$\Pr_{A \leftarrow \mathbb{Z}_q^{n \times m}} \left[\mathcal{A}(A, \vec{b}) \text{ outputs } \vec{s}' \text{ s.t. } A\vec{s}' = \vec{b} \right] = \text{negl}(n)$$

$\vec{s} \leftarrow [-B, B]^m$, $\vec{b} = A \cdot \vec{s}$

Goal: To show.

$$(A, \vec{b} \mid A \xleftarrow{\$} \mathbb{Z}_q^{n \times m}, \vec{s} \xleftarrow{\$} [-B, B]^m, \; b = A \cdot \vec{s})$$

is "close" to

$$(A, \vec{b} \mid A \xleftarrow{\$} \mathbb{Z}_q^{n \times m}, \vec{b} \xleftarrow{\$} \mathbb{Z}_q^{n \times 1})$$

Define SIS "hash" function as:

$$H_A(x) = A \cdot \vec{x} \pmod q$$

$$A \in \mathbb{Z}_q^{n \times m}, \; x \in [-B, B]^m$$

$K = [0 \ldots q-1]^{n \times m}$ Key distribution: samples uniformly from K.

Universal Hash Functions

Def. A hash function $H: K \times X \to Y$ is universal if $\forall x, x'$ s.t. $x \neq x'$

$$\Pr_{k \leftarrow K}[H_k(x) = H_k(x')] = \frac{1}{|Y|}$$

H.W. Show that the SIS hash function is universal.

Guessing Probability

$$\text{Guessing Prob}(X) = \max_{x \in X} \Pr_{x' \leftarrow X}[x' = x]$$

Let's say $\mathcal{X}$ is the uniform distribution on $[-B, \ldots B]^m$

$$G.P.(\mathcal{X}) = \frac{1}{(2B+1)^m}$$

Leftover Hash Lemma

(Simplified) (Impagliazzo-Lubin-Levy)

Let $H : K \times X \to Y$ be a universal hash function.

Let $\mathcal{X}$ be a distribution over X such that $G.P.(\mathcal{X}) \leq T$.

Then $\forall$ unbounded $\mathcal{D}$,

$$\left| \Pr_{\substack{k \leftarrow K \\ x \leftarrow \mathcal{X}}} [\mathcal{D}(k, H(k,x)) = 1] - \Pr_{\substack{k \leftarrow K \\ y \leftarrow Y}} [\mathcal{D}(k, y) = 1] \right| \leq T \cdot |Y|$$

$$T = \frac{1}{(2B+1)^{nm}} \longrightarrow \#\text{ possible values that } \vec{s} \text{ takes}$$

$$Y \to q^n$$

$$\left| \Pr[\mathcal{A}(\quad) = 1] - \Pr[\mathcal{A}(\quad) = 1] \right| \leq \frac{q^n}{(2B+1)^m}$$

LHL $\Rightarrow$ If SIS hash function is universal,

then $\left(A, \vec{b} \mid A \xleftarrow{\$} \mathbb{Z}_q^{n \times m}, \vec{s} \leftarrow [-B, B]^m, \vec{b} = A\vec{s}\right)$

and $\left(A, \vec{b} \mid A \xleftarrow{\$} \mathbb{Z}_q^{n \times m}, \vec{b} \xleftarrow{\$} \mathbb{Z}_q^n\right)$

are $\frac{q^n}{(2B+1)^m}$-close.

So far, SIS $\Rightarrow$ OWF.

SIS $\Rightarrow$ CRH

Collision Resistant Hash Functions. (CRHF)

A hash function $H : K \times X \to Y$ is a CRHF if:

① Compression: $|Y| < |X|$

② Collision-resistance:

$\forall$ nuPPT adversary $\mathcal{A}$,

$$\Pr_{k \leftarrow K}[\mathcal{A}(k) \text{ outputs } x \neq x' \text{ s.t. } H_k(x) = H_k(x')] = \text{negl}(|k|)$$

NOTE: Universal hash functions are not necessarily collision-resistant.

$\forall s_1, s_2$

$$\Pr_{A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}} \left[A \cdot s_1 = A \cdot s_2 \right] = \text{small}$$

Universal Hash

$\forall$ nu PPT Adv $\mathcal{A}$,

$$\Pr_{A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}} \left[\mathcal{A}(A) \to \vec{s}_1, \vec{s}_2 \text{ s.t. } A\vec{s}_1 = A\vec{s}_2 \right] = \text{negl}.$$

CR Hash

SIS hash function is collision resistant.

Homogenous SIS

$$\vec{b} = 0^{m \times 1}$$

Problem: Given A, find "short" $\vec{s}$ s.t. $A\vec{s} = 0$.

HW2

Inhomogenous SIS $\sim$ HSIS)

HSIS

$$\Pr_{A \xleftarrow{\$} \mathbb{Z}_q^{n \times m}}\left[\mathcal{A}(A) \text{ outputs "short" } \vec{s} \; \middle| \; A\vec{s} = 0 \right] = \text{negl}$$

CRHF.

Claim: SIS hash function is a CRHF.

P.T. Given A,
hard to find $\vec{s}_1, \vec{s}_2$ s.t.

$$A\vec{s}_1 = A \cdot \vec{s}_2 \pmod q$$

$$A(\vec{s}_1 - \vec{s}_2) = 0 \pmod q$$

This is a solution to HSIS!

Universal hash function:

$$f_a(x_1 \| x_2) = a x_1 + x_2$$

$$a \leftarrow \mathbb{Z}_q$$

Fix any x_1, x_2, x_1', x_2'

$$\Pr_a\left[a x_1 + x_2 = a x_1' + x_2' \right]$$

$$= \Pr_a\left[a(x_1 - x_1') = x_2' - x_2 \right]$$

$$= \Pr_a\left[a = \frac{(x_2' - x_2)}{(x_1 - x_1')} \right] = \frac{1}{q}$$